Commonwealth of Massachusetts
Executive Office for Administration and Finance
Information Technology Division

Policy Area: Security	**Policy #:** ITD-SEC-4.00
Title: Enterprise Cybercrime & Security Incident Response Policy and Procedures	**Effective Date:** February 6, 2003

Issue Statement
Commonwealth of Massachusetts agencies and organizations that reside within the security perimeter managed by the Information Technology Division (ITD), comprise the wide area network community known as MAGNet: the Massachusetts Access to Government Network. To optimize a secure community, MAGNet participants must be able to identify, report, and resolve cybercrime & security incidents in a manner that mitigates current and future risk to themselves and other potentially affected agencies or organizations. Cybercrime & Security Incidents are defined as internally or externally initiated events, intentional or accidental, that threaten or exploit an unauthorized and/or illegal use of Commonwealth electronic information systems and/or services. Such events include, but are not limited to, a criminal use of Commonwealth systems and/or services (e.g., cyber-stalking, identity theft, child pornography, etc.) as well as disclosure, destruction, and/or alteration of state managed systems or data.

The Commonwealth's Position
ITD supports agencies in their response to cybercrime & security incidents, by providing guidance, assistance, and recommendations that may include immediate countermeasure activities (e.g., deleting and/or isolating vulnerable or exploited elements, disabling individual and/or group access), referral to legal authorities, and other measures deemed necessary.

Cybercrime & security incidents, originating from, affecting, or potentially affecting Executive Department[1] agency(ies) and/or organization(s), must be reported to CommonHelp immediately. CommonHelp will establish a trouble ticket and initiate contact with ITD's Cybercrime Security and Incident Response Team (CSIRT) as well as other event-relevant ITD technical support groups. Following such incident notification, the reporting agency's designated contact must provide a report to ITD's CSIRT, via the exchange distribution list ITD-DL - CSIRT or CSIRT@state.ma.us , within five working days after the incident. A form is attached for use in reporting an incident. In cases where incident resolution is ongoing, a daily status report must be submitted. Executive Department agencies cannot report cybercrime and security incidents to law enforcement authorities until the agency has reported the incident to CommonHelp and, except in cases of imminent threat, received ITD's permission to contact the law enforcement authority.

Commonwealth Agency/Organization Responsibilities
The agency/organization head, or their designee, is responsible for ensuring this policy is communicated to employees and business partners. Agency/organization heads and their designees must ensure the following:

- Adequately trained and knowledgeable agency personnel are identified to work with ITD in reporting and resolving cybercrime & security incidents. The primary and/or secondary IT contact(s), within the Contact Application, will be the designated person(s) responsible for reporting cybercrime & security incidents. To access and enter/maintain the designated IT personnel's information into CommonHelp's Contact Application, logon to <http://www.itd.state.ma.us/ContactApp/index.asp>.
- Designated IT personnel must be able to make immediate technical and managerial decisions for the agency/organization, which are necessary to protect affected or potentially affected, IT environments.

[1] The Executive Department is comprised of the Executive Branch minus the Constitutional Offices, (i.e., the State Auditor, State Treasurer, Attorney General and Secretary of the Commonwealth.)

- Development of any local agency/organization Cybercrime & Security Incident Response policies must conform to this policy.
- Designated IT personnel, including agency/organization senior technical managers, are members of the IT.Notices listserver email communication group, to ensure their timely receipt of information regarding viruses, hacks and other potential threats. To join IT.Notices send a blank email to join-IT.Notices@listserv.state.ma.us
- Should a cybercrime & security incident occur, the affected agency/organization is expected to collaborate with ITD to protect both the agency/organization and Commonwealth enterprise IT environments, as well as to determine whether the incident must be reported to other state and/or legal authorities.

When a cybercrime & security incident has, or is occurring in the form of an attack intrusion, the agency/organization designated IT personnel, who have previously been identified to CommonHelp's Contact Application, shall act in conformance with CommonHelp's Attack Intrusion Notification Procedures, found at http://www.itd.state.ma.us/HelpDesk/Publications/AttackNotificationProcedures.htm and shall:

- Start an event log by noting date and time of all actions taken,
- Investigate, and identify relevant findings,
- Identify risk to specific systems and/or information assets,
- If findings reflect that a reportable incident did not occur, or the facts were indeterminate, participants will log and share knowledge with networking manager/administrator, and ITD's CSIRT,
- If findings confirm a reportable incident, notify designated agency and ITD Cybercrime & Security Incident Response Team (ITD-DL - CSIRT) and CommonHelp,
- Take snapshot of pertinent files within the first half hour of incident investigation,
- Confer with networking manager/administrator and ITD's CSIRT,
- Formulate and implement response plans as soon as possible following incident discovery,
- Notify management and ITD's CSIRT of significant incident and response plans,
- Monitor and evaluate the situation,
- Prepare (or assist in preparing) and file preliminary and final reports with appropriate agency personnel and ITD's CSIRT,
- Preserve evidence, and
- Conduct a post-mortem and apply lessons learned.

Compliance

Agencies within the Executive Department must comply with this Enterprise Cybercrime & Security Incident Response Policy. All Commonwealth agencies and organizations must comply with this policy as a prerequisite for access to and/or participation within MAGNet, and/or to use information resources managed by ITD. Vendors, who seek to work with any agency or organization within the Commonwealth of Massachusetts, must comply with this and all the Commonwealth's Enterprise Security Policies, Standards and Procedures as published by ITD.

Supplementary Information

- Cybercrime & Security Incident Response Form (Appendix A)
- Enterprise Security Policies
  http://www.itd.state.ma.us/spg/publications/standards/index.htm
- ITD's Attack Intrusion Notification Procedures
  http://www.itd.state.ma.us/HelpDesk/Publications/AttackNotificationProcedures.htm

Points of Contact

- Cybercrime & Security Incident Response Team CSIRT@state.ma.us
- CommonHelp (866)888-2808 commhelp@state.ma.us ITD-DL - COMMON HELP
- Chief Information Security Officer, ITD
- Enterprise Security Board
- General Counsel, ITD

Cybercrime & Security Incident Response Form

Date_____
Name of Person Reporting Incident_____
Agency MMARS Code_____

Date/Time CommonHelp was contacted (Include ticket number)_____

Date/Time/Person at Agency contacted_____

Description of threat or incident_____

Is the incident continuing? _____

How did the incident commence? _____

IT assets being compromised, including identification and classification (i.e., level of confidentiality) of affected data or systems
_____

Has the agency determined the cause and origination of the incident? If so, please describe
_____

List actions, which must be and/or have been taken to stop and/or remedy the incident
_____

Detail the resources, which must be used to stop and/or remedy the situation_____
_____

Detail steps, which have been taken to mitigate or remediate the damage_____
_____

List evidence, which is available to assist in the investigation (e.g., log files)_____
_____